CLAIMS

WHAT IS CLAIMED IS:

1. A computer system, comprising:

a bus;

a memory coupled to the bus, wherein the memory includes a plurality of storage locations, wherein the plurality of storage locations are divided into a plurality of memory units; and

a device coupled to access the memory over the bus, wherein the device includes one or more locks configured to control access to one or more of the plurality of memory units.

2. The computer system of claim 1, wherein the bus is configured to operate according to an LPC bus protocol.

3. The computer system of claim 1, wherein the memory is a ROM.

4. The computer system of claim 3, wherein the ROM is a BIOS ROM.

5. The computer system of claim 1, wherein the device is a south bridge.

6. The computer system of claim 1, wherein the locks include a plurality of registers, wherein one or more entries in one or more of the plurality of registers indicate an access control setting for one or more of the memory units.

7. The computer system of claim 6, wherein at least one of the plurality of registers is configured to store three locking bits for one of the memory blocks, wherein the three locking

bits include a read lock bit, a write lock bit, and a lock-down bit, wherein the read lock bit and the write lock bit are permanent until reset when the lock-down bit is set.

8. The computer system of claim 6, wherein at least one of the plurality of registers is configured to store eight bits, wherein the eight bits include three locking bits for one of the memory blocks and another three locking bits for another one of the memory blocks, wherein the three locking bits include a first read lock bit, a first write lock bit, and a first lock-down bit, wherein when the first lock-down bit is set, the first read lock bit and the first write lock bit are permanent until reset, and wherein the another three locking bits include a second read lock bit, a second write lock bit, and a second lock-down bit, wherein when the second lock-down bit is set, the second read lock bit and the second write lock bit are permanent until reset.

9. The computer system of claim 8, wherein the at least one of the plurality of registers is configured with bit 0 as the first write lock bit, bit 1 as the first lock-down bit, bit 2 as the first read lock bit, bit 4 as the second write lock bit, bit 5 as the second lock-down bit, and bit 6 as the first read lock bit.

10. A memory, comprising:

a first plurality of storage locations configured with BIOS data; and

a second plurality of storage locations, wherein the second plurality of storage locations includes:

a first plurality of blocks readable only in SMM; and

a second plurality of blocks readable in SMM and at least one operating mode other than SMM.

11. The memory of claim 10, wherein the at least one counter comprises a monotonic counter.

12. The memory of claim 10, wherein the second plurality of storage locations further includes:
at least one counter stored in a flat memory space.

13. The memory of claim 12, wherein the first plurality of blocks includes a block with a write once lock.

14. The memory of claim 12, wherein the first plurality of blocks includes a block with a never erase lock.

15. The memory of claim 12, wherein the first plurality of blocks includes a block that can be written in SMM and in at least one operating mode other than SMM.

16. The memory of claim 12, wherein the second plurality of blocks includes a block with a write once lock.

17. The memory of claim 12, wherein the second plurality of blocks includes a block with a never erase lock.

18. The memory of claim 12, wherein the plurality of blocks includes a block that can be written in SMM and in at least one operating mode other than SMM.

19. The memory of claim 10, wherein the first plurality of storage locations are addressed in an address range including from FFFF,FFFFh to FFC0,0000h.

20. The memory of claim 10, wherein the second plurality of storage locations are addressed in an address range including from FFBF,FFFFh to FFB0,0000h

21. A method for operating a computer system, the method comprising:

requesting a memory transaction for one or more memory addresses;

determining a lock status for the one or more memory addresses;

returning the lock status for the one or more memory addresses;

determining if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed;

changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

22. The method of claim 21, wherein determining a lock status includes reading a first lock bit; and wherein returning the lock status includes returning the value of the first lock bit.

23. The method of claim 22, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

24. The method of claim 23, wherein changing the lock status of the one or more memory addresses to allow the memory transaction includes changing the value of the first lock bit.

25. A method of operating a computer system, the method comprising:

issuing a request from a first device for a memory transaction for a memory location;

receiving the request for the memory transaction at a second device that does not include the memory location or a copy of the contents of the memory location;

returning a response from the second device to the first device issuing the request for the memory transaction.

26. The method of claim 25, wherein returning the response from the second device includes ending the memory transaction without the memory transaction reaching the memory location.

27. The method of claim 25, further comprising:

ending the request for the memory transaction without the memory location responding to the request for the memory transaction.

28. The method of claim 25, wherein the second device includes a bridge coupled between the first device and the memory location, wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the bridge to the first device issuing the request for the memory transaction.

29. The method of claim 28, wherein said returning the response from the bridge to the first device issuing the request for the memory transaction includes responding from an access filter within the bridge with a predetermined value upon receipt of the request for the memory transaction for the memory location, when the computer system is operating in a first operating mode.

30. The method of claim 29, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a ROM.

31. The method of claim 29, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a flash memory.

32. The method of claim 25, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a memory.

33. The method of claim 25, wherein the first device includes security hardware, wherein said receiving the request for the memory transaction at the second device that does not include the memory location or the copy of the contents of the memory location includes receiving the request for the memory transaction at the security hardware within the first device; and wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes

returning the response from the security hardware to the first device issuing the request for the memory transaction.

34. The method of claim 25, further comprising:

reading a first value from a memory location within the second device before returning the response, wherein the memory location within the second device is different from the memory location for the memory transaction.

35. A computer system, comprising:

means for requesting a memory transaction for one or more memory addresses;

means for determining a lock status for the one or more memory addresses;

means for returning the lock status for the one or more memory addresses;

means for determining if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed;

means for changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

36. The computer system of claim 35, wherein the means for determining the lock status comprises means for reading a first lock bit; and wherein the means for returning the lock status includes means for returning the value of the first lock bit.

37. The computer system of claim 36, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

38. The computer system of claim 37, wherein the means for changing the lock status of the one or more memory addresses to allow the memory transaction includes means for changing the value of the first lock bit.

39. A computer system, comprising:

means for issuing a request from a first device for a memory transaction for a memory location;

means for receiving the request for the memory transaction at a second device that does not include the memory location or a copy of the contents of the memory location; and

means for returning a response from the second device to the first device issuing the request for the memory transaction.

40. The computer system of claim 39, wherein the means for returning the response from the second device includes means for ending the memory transaction without the memory transaction reaching the memory location.

41. The computer system of claim 39, further comprising:

means for ending the request for the memory transaction without the memory location responding to the request for the memory transaction.

42. The computer system of claim 39, wherein the second device includes a bridge coupled between the first device and the memory location, wherein the means for returning the response from the second device to the first device issuing the request

for the memory transaction includes means for returning the response from the bridge to the first device issuing the request for the memory transaction.

43. The computer system of claim 42, wherein the means for returning the response from the bridge to the first device issuing the request for the memory transaction includes means for responding from an access filter within the bridge with a predetermined value upon receipt of the request for the memory transaction for the memory location, when the computer system is operating in a first operating mode.

44. The computer system of claim 43, wherein the means for issuing the request from the first device for the memory transaction for the memory location includes means for issuing the request from the first device for the memory transaction for the memory location in a ROM.

45. The computer system of claim 43, wherein the means for issuing the request from the first device for the memory transaction for the memory location includes means for issuing the request from the first device for the memory transaction for the memory location in a flash memory.

46. The computer system of claim 39, wherein the means for issuing the request from the first device for the memory transaction for the memory location includes means for issuing the request from the first device for the memory transaction for the memory location in a memory.

47. The computer system of claim 39, wherein the first device includes security hardware, wherein the means for receiving the request for the memory transaction at the second device that does not include the memory location or the copy of the contents of the memory location includes means for receiving the request for the memory transaction at the security hardware within the first device; and wherein the means for returning the response from the second device to the first device issuing the request for the memory transaction includes means for returning the response from the security hardware to the first device issuing the request for the memory transaction.

48. The computer system of claim 39, further comprising:

means for reading a first value from a memory location within the second device before returning the response, wherein the memory location within the second device is different from the memory location for the memory transaction.

49. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:

requesting a memory transaction for one or more memory addresses;

determining a lock status for the one or more memory addresses;

returning the lock status for the one or more memory addresses;

determining if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed;

changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

50. The computer readable program storage device of claim 49, wherein determining a lock status includes reading a first lock bit; and wherein returning the lock status includes returning the value of the first lock bit.

51. The computer readable program storage device of claim 50, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

52. The computer readable program storage device of claim 51, wherein changing the lock status of the one or more memory addresses to allow the memory transaction includes changing the value of the first lock bit.

53. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:

issuing a request from a first device for a memory transaction for a memory location;

receiving the request for the memory transaction at a second device that does not include the memory location or a copy of the contents of the memory location;

returning a response from the second device to the first device issuing the request for the memory transaction.

54. The computer readable program storage device of claim 53, wherein returning the response from the second device includes ending the memory transaction without the memory transaction reaching the memory location.

55. The computer readable program storage device of claim 53, the method further comprising:

ending the request for the memory transaction without the memory location responding to the request for the memory transaction.

56. The computer readable program storage device of claim 53, wherein the second device includes a bridge coupled between the first device and the memory location, wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the bridge to the first device issuing the request for the memory transaction.

57. The computer readable program storage device of claim 56, wherein said returning the response from the bridge to the first device issuing the request for the memory transaction includes responding from an access filter within the bridge with a predetermined value upon receipt of the request for the memory transaction for the memory location, when the computer system is operating in a first operating mode.

58. The computer readable program storage device of claim 57, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a ROM.

59. The computer readable program storage device of claim 57, wherein said issuing the request from the first device for the memory transaction for the memory location

includes issuing the request from the first device for the memory transaction for the memory location in a flash memory.

60. The computer readable program storage device of claim 53, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a memory.

61. The computer readable program storage device of claim 53, wherein the first device includes security hardware, wherein said receiving the request for the memory transaction at the second device that does not include the memory location or the copy of the contents of the memory location includes receiving the request for the memory transaction at the security hardware within the first device; and wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the security hardware to the first device issuing the request for the memory transaction.

62. The computer readable program storage device of claim 53, the method further comprising:

reading a first value from a memory location within the second device before returning the response, wherein the memory location within the second device is different from the memory location for the memory transaction.